

(19)



Bureau voor de
Industriële Eigendom
Nederland

(11) 1007409

(12) C OCTROOI⁶

(21) Aanvraag om octrooi: 1007409

(51) Int.Cl.⁶
H04L9/32, H04L9/08, H04Q7/32

(22) Ingediend: 31.10.97

(41) Ingeschreven:
18.11.97 I.E. 98/02

(47) Dagtekening:
18.11.97

(45) Uitgegeven:
02.02.98 I.E. 98/02

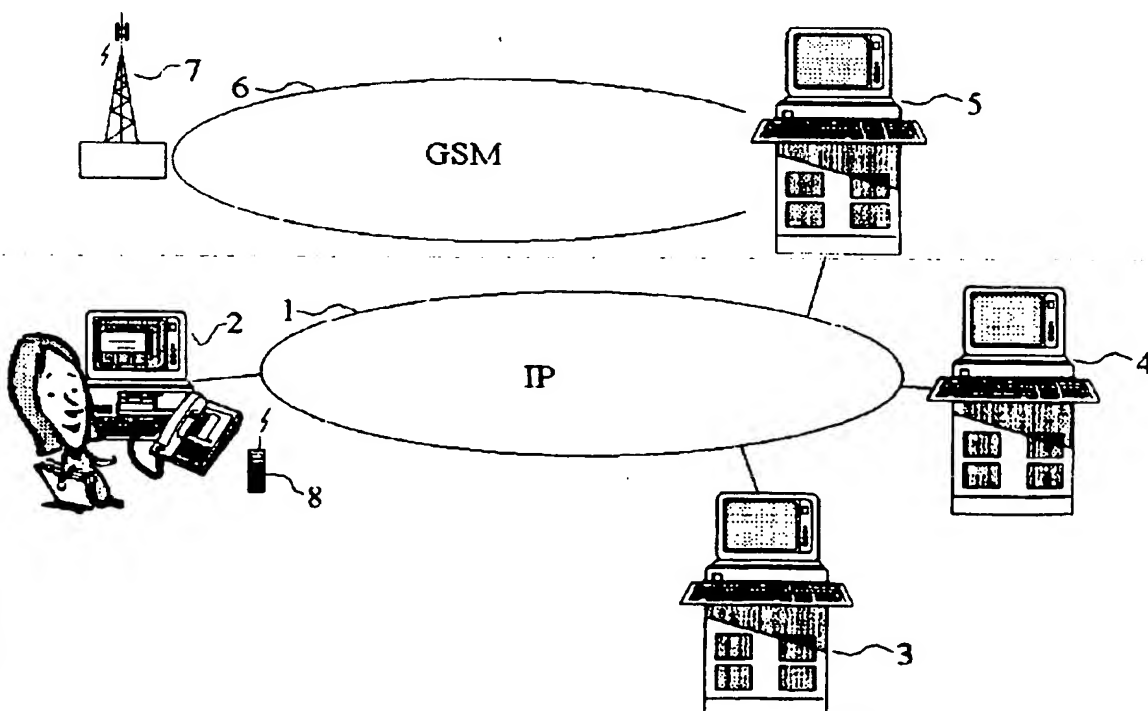
(73) Octrooihouder(s):
Koninklijke PTT Nederland N.V. te Groningen.

(72) Uitvinder(s):
Sharon Christie Lesley Prins te Groningen

(74) Gemachtigde:
Ir. G.J. Baas te 2509 CH Den Haag.

(54) Authenticatiesysteem.

(57) Authenticatiesysteem, waarbij een gebruiker van een systeem zich authenticceert tegenover dat systeem (3) door middel van het bij dat systeem invoeren van een authenticatiecode, welke door het systeem op geldigheid wordt onderzocht. De authenticatiecode wordt door een generator (4) gegenereerd en wordt enerzijds aan het systeem overgedragen dat om authenticatie vraagt. Anderzijds wordt de code aan de gebruiker overgedragen, door het te adresseren aan een uniek, door de gebruiker opgegeven adres. Uiteraard dient het overdrachtsmedium "intruder proof" te zijn. Bij voorkeur wordt gebruik gemaakt van een strikt persoonlijke gebruikersterminal, zoals een (GSM) terminal die is voorzien van een "Security & Identification Module" (SIM).



NL C 1007409

De inhoud van dit octrooi komt overeen met de oorspronkelijk ingediende beschrijving met conclusie(s) en eventuele tekeningen.

Best Available Copy

Authenticatiesysteem

ACHTERGROND VAN DE UITVINDING

De uitvinding heeft betrekking op een authenticatiesysteem, waarbij een gebruiker van een systeem zich authenticceert tegenover dat systeem door middel van het bij dat systeem invoeren van een
5 authenticatiecode, welke door het systeem op geldigheid wordt onderzocht.

Een dergelijk authenticatiesysteem is van algemene bekendheid. Vaak worden voor authenticatie alfanumerieke "passwords" gebruikt, die door de gebruiker worden ingetoetst. Als een vast password wordt gebruikt,
10 heeft dat het bezwaar dat het password ontvreemd of gecopieerd en daarna misbruikt kan worden. Om die reden bestaan er ook "one time password" (OTP) systemen, waarbij een password slechts één keer wordt gebruikt.

15 SAMENVATTING VAN DE UITVINDING

De uitvinding voorziet in een OTP systeem waarbij het OTP, dat door een OTP generator gegenereerd wordt, enerzijds aan het systeem wordt overgedragen dat om authenticatie vraagt, en dat anderzijds aan de gebruiker wordt overgedragen, waarbij het OTP wordt geadresseerd aan
20 een uniek gebruikersadres. Uiteraard dient het overdrachtsmedium "intruder proof" te zijn. Bij voorkeur wordt gebruik gemaakt van een strikt persoonlijke gebruikersterminal, zoals een (GSM) terminal die is voorzien van een "Security & Identification Module" (SIM).

De uitvinding zal hierna aan de hand van een uitvoeringsvoorbeeld
25 nader worden uiteengezet.

UITVOERINGSVOORBEELD

Figuur 1 toont zeer schematisch een uitvoeringsvoorbeeld van de uitvinding. Op een voor IP geschikt netwerk 1 (internet) is een
30 terminal 2 aangesloten, een server 3 en een authenticatieserver 4. Op een voor GSM geschikt netwerk 6 is een "Short Message Service" (SMS) server 5 aangesloten en een basisstation 7, die verbinding kan maken met een GSM terminal 8. Uiteraard zijn er in werkelijkheid veel meer terminals, servers etc.

35 De werking van het authenticatiesysteem volgens de uitvinding, uitgevoerd in het in figuur 1 getoonde stelsel is als volgt.

1007409

Een gebruiker maakt via terminal 2 en het internet 1 verbinding met server 3 om daar van een service gebruik te maken waarvoor authenticatie nodig is. De server 3 stuurt daartoe een HTML gecodeerd bericht naar de terminal, waarin de gebruiker verzocht wordt het

5 telefoonnummer van haar mobiele telefoon 8 in te voeren. De server 3 verstuurt een verzoek naar authenticatieserver 4 om een (random) authenticatiecode te genereren en naar de gebruiker te doen uitzenden. Daarna zendt de server 3 aan de gebruiker het verzoek om te wachten op een op haar mobiele telefoontoestel te ontvangen SMS-bericht met de

10 gevraagde authenticatiecode. Intussen wordt die code door server 4 gegenereerd en naar zowel SMS server 5 als naar server 3 verstuurd. De SMS server 5 verzendt de code, in de vorm van een SMS-bericht, naar het mobiele telefoontoestel 8, dat de ontvangen code op het

beeldschermje toont. De gebruiker leest dat en geeft de code via haar

15 terminal aan de server 3 door. Deze vergelijkt de van de terminal 2 ontvangen code met de (direct) van de server 4 ontvangen code. Bij overeenstemming wordt de door de gebruiker gevraagde service vrijgegeven.

Opgemerkt wordt dat de links tussen de servers 3, 4 en 5 wel veilig

20 dienen te zijn. Het kunnen (anders dan de figuur aangeeft) verbindingen buiten het IP net zijn of wel via het IP net gerealiseerd zijn, maar dan beveiligd, bijvoorbeeld door "firewalls" etc. Server 4 kan ook geïncorporeerd zijn in server 3, hetgeen de veiligheid eveneens verhoogt.

25 In plaats van een telefoontoestel, kan ook gebruik gemaakt worden van andere soorten ontvangers, bijvoorbeeld een paging-ontvanger. Dit soort ontvangers is heden ten dage echter minder "intruder-proof" dan de huidige GSM-terminals. Ook is het niet persé nodig om van een radio-ontvanger gebruik te maken: elk medium is geschikt, mits de

30 "link" van de codegenerator (authenticatieserver) naar de ontvanger bij de gebruiker voldoende veilig is. In principe kan als medium hetzelfde medium worden gebruikt als waarmee de terminal verbinding heeft met de server (3) die om authenticatie vraagt. Als medium kan bijvoorbeeld een beveiligd virtueel kanaal of een "Virtual Private

35 Network" (VPN) worden gebruikt.

In het bovenstaande wordt voorgesteld dat de gebruiker de ontvangen authenticatiecode afleest (van het scherm van haar GSM toestel) en aan de server 3 doorgeeft door die code via haar toetsenbord over te

typen. Op zich is het natuurlijk fraaier om de op de gebruikerlocatie ontvangen authenticatiecode direct naar de server 3 te verzenden zonder die te hoeven overtypen. Bijvoorbeeld zou dat kunnen door een lokale, directe dataverbinding te gebruiken tussen de GSM-ontvanger en de dataterminal 2. De dataterminal kan --via een daartoe geëigend applicatieprogramma-- de ontvangen authenticatiecode inlezen en aan server 3 doorgeven. Ook kan de authenticatiecode-ontvanger 8 in de terminal 2 geïncorporeerd worden. Wanneer hetzelfde medium zou worden gebruikt als voor de verbinding tussen de terminal 2 en de server 3, in casu het internet 1, ligt een dergelijke directe doorgifte van de lokaal ontvangen authenticatiecode nog meer voor de hand. Het proces is dan:

- server 3 vraagt terminal 2 om authenticatiecode;
- server 3 verzoekt server 4 om een authenticatiecode te genereren;
- 15 - server 4 genereert een authenticatiecode en zendt die naar server 3 en naar een gebruikersterminal: in het voorgaande dus via GSM-SMS (server 5, netwerk 6 en radioverbinding 7-8), of, als alternatief, via een "secure" verbinding via het IP netwerk 1, naar de terminal 2;
- de lokale gebruiker neemt de ontvangen authenticatiecode over en
- 20 zendt die naar server 3; bij een directe lokale koppeling wordt de authenticatiecode lokaal ontvangen, via GSM of via IP, en nadien door de terminal 2 naar server 3 gezonden; in dat laatste geval hoeft de gebruiker dus niets te doen; zelfs kan het authenticatieproces voor de gebruikere "onder water" plaatshebben.

CONCLUSIES

1. Authenticatiesysteem, waarbij een lokale gebruiker zich tegenover een systeem authenticceert door het, via een lokale terminal (2), bij dat systeem invoeren van een authenticatiecode, die door dat systeem op geldigheid wordt onderzocht, met het kenmerk dat de authenticatiecode gegenereerd wordt door een codegenerator (4), die de gegenereerde code enerzijds overgedraagt aan het systeem (3) dat om authenticatie vraagt, en anderzijds adresseert en overdraagt aan een lokale code-ontvanger (8) met een eigen ontvangstadres, waarna de gebruiker de aldus ontvangen authenticatiecode aan het daarom vragende systeem (3) overdraagt.
2. Authenticatiesysteem volgens conclusie 1, met het kenmerk dat de lokale code-ontvanger een lokale verbinding heeft met de genoemde lokale terminal (2).
3. Authenticatiesysteem volgens conclusie 1, met het kenmerk dat de lokale code-ontvanger deel uitmaakt van de lokale terminal (2).
4. Authenticatiesysteem volgens conclusie 1, met het kenmerk dat voor de verbinding tussen de lokale terminal (2) en de server (3) enerzijds, en de verbinding tussen de codegenerator (4) en de lokale code-ontvanger (8) anderzijds, gebruik wordt gemaakt van verschillende media (1, 6).
5. Authenticatiesysteem volgens conclusie 1, met het kenmerk dat voor de verbinding tussen de lokale terminal (2) en de server (3) enerzijds, en de verbinding tussen de codegenerator (4) en de lokale code-ontvanger (8) anderzijds, gebruik wordt gemaakt van hetzelfde, gemeenschappelijke medium, zij het van verschillende kanalen binnen datzelfde medium.
6. Authenticatiesysteem volgens conclusie 4, met het kenmerk dat de lokale code-ontvanger gevormd wordt door een mobiele spraak- of dataterminal.
7. Authenticatiesysteem volgens conclusie 6, met het kenmerk dat de lokale code-ontvanger wordt gevormd door een digitale mobiele terminal, zoals een GSM-terminal.
8. Authenticatiesysteem volgens conclusie 4, met het kenmerk dat de lokale code-ontvanger wordt gevormd door een paging-terminal.

